



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/438,342	11/11/1999	GREGORY G. ROSE	PA990055	9169

23696 7590 10/02/2003

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER

MCARDLE, JOSEPH M

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 10/02/2003

8

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/438,342

Applicant(s)

ROSE, GREGORY G.

Examiner

Joseph McArdle

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 8-10, 14-16, 20-22, 26, 27 and 29 is/are rejected.
- 7) ☒ Claim(s) 5-7, 11-13, 17-19, 23-25, 28, 30 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 November 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 2, 4, 14, 16, and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Jansen (6587562). In regards to claim 1, Jansen discloses a synchronous stream cipher design in column 1, lines 25-45, that comprises encryptor and decryptor stations made up of data-stream generators that are used to generate and transmit a plurality of data streams that contain control data. Jansen further discloses in column 4, lines 30-37, and 55-63, that control generators having clock trigger inputs are used to determine when the data stream generator will cycle its data from a linear feedback shift register. It is this generated control data that will allow a recipient to determine the current state of a stream cipher, which is called for under claim 1.

3. In regards to claim 2, Jansen's disclosure of control data and clock trigger inputs disclosed above meets the limitations of claim 2, which calls for including a cycle number in the control set of numbers.

4. In regards to claims 4 and 16, Jansen discloses in column 6, lines 22-41, that linear feedback shift registers use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. This meets the limitations of claim 4 and 16, which call for determining the current state of the stream cipher by using the polynomial of claims 4 and 16.

5. In regards to claim 14, Jansen discloses in column 1, lines 55-67, and column 2, line 1, that non-linearity is introduced into the system by using a linear feedback shift register to irregularly clock one of the data generators. Claim 14 calls for including a stutter number in the control set of numbers. The stutter number of claim 14 was described in the specification as a means to introduce non-linearity into the data stream, therefor Jansen's disclosure meets the limitations of claim 14.

6. In regards to claim 26, Jansen discloses a synchronous stream cipher design in column 1, lines 25-45, that comprises encryptor and decryptor stations made up of data-stream generators that are used to generate and transmit a plurality of data streams which contain control data. Jansen further discloses in column 4, lines 30-37, and 55-63, that control generators having clock trigger inputs are used to determine when the data stream generator will cycle its data from a linear feedback shift register. Jansen discloses in column 1, lines 55-67, and column 2, line 1, that non-linearity is introduced into the system by using a linear feedback shift register to irregularly clock one of the data generators. Jansen's disclosure of the control generator used to control the

cycling of data from the linear feedback shift register and the use of another linear feedback shift register that injects non-linearity into the data stream will allow a recipient to determine the current state of the stream cipher as called for under claim 26

7. Claim 27 is rejected under 35 U.S.C. 102(e) as being anticipated by Raith (5546464). Raith discloses a design in column 5, lines 49-54, that allows mobile stations and base stations to synchronize their ciphered data streams. Raith further discloses in column 12, lines 3-23, that in order for a receiver to generate the correct cipher stream, the transmitter and receiver must use the same key-stream generator and that the transmitter and receiver must be in sync. Raith further discloses that synchronization is made possible by transmitting from the transmission station to the receiving station the contents of internal memory devices, which include counters that indicate the status of the cipher at the transmission source, and using these counter values to determine the state of the stream cipher at the reception site. This meets the limitations of claim 27, which calls for generating stream ciphers based upon a common recurrence relation which comprises transmitting an offset from a transmission site to a reception site in order to allow to reception site to determine the current state of the stream cipher.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 3 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jansen in view of Raith (5546464). Jansen's design disclosed above meets all of the aforementioned limitations of claims 2 and 14 above. However, Jansen's design does not mention transmitting from a mobile station to a base station. Raith discloses in column 12, lines 24-28, that synchronization can be obtained when transmissions are made in either direction between mobile stations and base stations. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Raith's teachings on the use of transmitting between mobile stations and base stations into Jansen's design in order to achieve a design that is capable of transmitting from a mobile station to a base station.

10. Claims 8 –10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jansen in view of Bright (4893339). In regards to claims 8, 9, 20, and 21, Jansen's design described above meets all of the aforementioned limitations of claims 2 and 14. However, Jansen's design does not mention transmitting the encrypted data stream to a plurality of recipients whereby each recipient uses the control data containing the cycle numbers to determine a different current state of the

stream cipher. Bright discloses in column 3, lines 12-24, a transmission system that comprises a base station and a plurality of remote units. Bright further discloses in column 4, lines 27-35, that a plurality of synchronization signals may be used, each of which may indicate a particular group of recipients. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Bright's teachings on the use of transmitting to a plurality of recipients into Jansen's design in order to achieve a design that transmits encrypted data from a source to a plurality of recipients, whereby each recipient uses the control data contained within the encrypted data to determine a different current state of the stream cipher.

11. In regards to claims 10, and 22 Jansen further discloses in column 6, lines 22-41, that linear feedback shift registers use polynomials of various degree and that these polynomials represent the bit shifting operations that occur during a ciphering process. This meets the limitations of claim 4, which calls for determining the current state of the stream cipher by using the polynomial of claims 10 and 22.

12. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Raith in view of Jansen. Raith's design disclosed in the rejection of claim 27 above provides a means for synchronizing two stream ciphers based upon a common recurrence relation in which an offset is transmitted from a transmission site to a reception site allowing the reception site to determine the current state of the stream cipher. However Raith's design makes no mention of using linear feedback shift registers for outputting the

Art Unit: 2132

stream ciphers. Jansen discloses in column 1, lines 51-58, that linear feedback shift registers are used to generate output data streams. Jansen further describes in column 4, lines 30-41, that a control generator is used to control the clocking of the linear feedback shift register, and that control data is used to indicate the status of the stream cipher at the transmission source. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Jansen's teachings on the use of linear feedback shift registers and control generators into Raith's design in order to achieve a design that is capable of using a linear feedback shift register for outputting stream cipher data and control data in order to allow a reception site to determine the current state of the stream cipher.

Allowable Subject Matter


13. Claims 5-7, 11-13, 17-19, 23-25, 28 and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

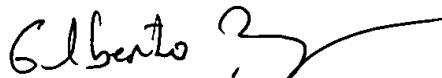
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



Joseph McArdle
Examiner
Art Unit 2132

jmm



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100